UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/552,951	04/20/2000	Zheng Jia	109905-136719	6045

25943 7590 07/12/2004

SCHWABE, WILLIAMSON & WYATT, P.C.
PACWEST CENTER, SUITES 1600-1900
1211 SW FIFTH AVENUE
PORTLAND, OR 97204

EXAMINER	
CURCIO, JAMES A F	

ART UNIT	PAPER NUMBER
2132	12

DATE MAILED: 07/12/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/552,951	Applicant(s) JIA ET AL.	
	Examiner James Curcio	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 March 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13,17 and 19-27* is/are pending in the application.

4a) Of the above claim(s) ~~*14-16 and 18*~~ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) ~~1-27~~ 1-13, 17 and 19-27 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. The amendment filed March 31, 2004 is objected to under 35 U.S.C. 132 because it introduces new matter into the disclosure. 35 U.S.C. 132 states that no amendment shall introduce new matter into the disclosure of the invention. The added material which is not supported by the original disclosure is as follows: "second obscuring instructions" in claims 1, 10, 19, and all claims depending therefrom and "runtime manager" and injecting and encrypting steps involving the "runtime manager" in claims 6, 20, 27, and all claims depending therefrom.

2. Applicant is required to cancel the new matter in the reply to this Office Action. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

3. Claim 1-13; 17, 19-20, and 24-27 rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contain subject matter, which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. The added material that is not supported by the original disclosure is as follows: "second obscuring instructions" in independent claims 1, 10, 19, and all claims depending therefrom and "runtime manager" and injecting and encrypting steps involving the "runtime manager" in claims 6, 20, 27, and all claims depending therefrom.

Response to Arguments

4. The amendments filed March 31, 2004 are insufficient to overcome the rejection of claims 1, 2, and 19 based upon Aucsmith et al (US 5892899A) applied under 35 U.S.C. 102 as set forth in the last Office action for the following reasons:

5. As per claims 1 and 19, Aucsmith et al discloses the following steps:

preparation of first obscuring instructions (column 1, lines 46-57; column 4, lines 16-20; column 5, lines 38-46; column 7, lines 9-15 and 23-25);

serializing the sequence of computer instructions (column 1, lines 46-57; column 4, lines 16-20; column 5, lines 38-46; column 7, lines 9-15 and 23-25);

the injection of second obscuring instructions into the serialized sequence of computer instructions in an automated process, using the first obscuring instructions (column 1, lines 46-57; column 4, lines 16-20; column 5, lines 38-46; column 7, lines 9-15 and 23-25; column 10, lines 62-65).

These steps are taught as being combined on a computer system and an embedded controller in two example embodiments (column 11, lines 42-47 and lines 66-67; column 12, lines 1-3), and this office action interprets the obscured sequences of instructions generated as comprising the instructions claimed in all of these steps combined.

6. As per claim 2, in addition to the teachings applied above, Aucsmith et al discloses the execution of the serialized sequence of computer instructions injected with

the second obscured instructions, one instruction at a time (column 5, lines 32-33 and column 9, lines 41-43).

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

8. Claims 1-5, 19, and 21 rejected under 35 U.S.C. 102(b) as being anticipated by Aucsmith et al (US5892899A).

9. As per claims 1 and 19, Aucsmith et al discloses the preparation of obscuring instructions (column 1, lines 46-57; column 4, lines 16-20; column 5, lines 38-46; column 7, lines 9-15 and 23-25), the injection of these obscuring instructions into computer code to form an obscured sequence of instructions (column 1, lines 46-57; column 4, lines 16-20; column 5, lines 38-46; column 7, lines 9-15 and 23-25), and the encryption of a static image of this sequence (column 10, lines 62-65). These steps are taught as being combined on a computer system and an embedded controller in two example embodiments (column 11, lines 42-47 and lines 66-67; column 12, lines 1-3), and this office action interprets the obscured sequence of instructions generated as comprising the instructions taught in all of these steps combined.

10. As per claim 2, in addition to the teachings applied above, Aucsmith et al discloses the execution of obscured instructions one instruction at a time (column 5, lines 32-33 and column 9, lines 41-43).

11. As per claim 3, in addition to the teachings applied above, Aucsmith et al discloses the transformation of a first set of codes into a second set of obscuring instruction identification codes (see the method of choosing mutations by cycling through the pseudo-random keys in column 5, lines 38-46). The invention also discloses the generation of the second obscuring instructions . . . (see "obfuscated subprograms cyclically mutate" in column 5, lines 38-46).

12. As per claims 4-5, in addition to the teachings applied above, while Aucsmith et al fails to explicitly state that the first set of obscuring instruction identification codes is a set of numeric values, the "pseudo-random keys" (column 5, lines 38-46) are encoded in a computer system (column 3, lines 28-33) and therefore are inherently represented with binary numbers. Aucsmith et al discloses that said generating of the second set of obscuring instruction identification codes comprise performing a mathematical transformation on the numeric values of the first set of obscuring identification codes to produce the numeric values of the second set of obscuring instruction identification codes (column 3, lines 28-33 and column 5, lines 38-46). The transformations in Aucsmith et al are mathematical because transformations of binary numbers on a computer system are inherently mathematical. Aucsmith et al also discloses injecting into the serialized sequence of instructions injected with the second obscuring instructions, a description of the mathematical transformation performed (column 3,

lines 28-33 and column 5, lines 38-46; see also working matrix M2 containing Boolean functions to recover the plaintext of the obfuscated subprograms in column 6, lines 57-64. This matrix is a compressed form of the record of transformation).

13. As per claim 21, in addition to the teachings applied above, Aucsmith et al also discloses an obscuring obstruction bank . . . (see "pattern(s) of mutations" in column 4, lines 16-20; column 5, lines 37-38 and lines 40-41; column 7, lines 9-16 and 23-25), a transformation function bank . . . (see "predetermined mutation partnership function" in column 5, lines 39-41), and a generator to generate blocks of obscuring instructions by selecting identification codes of the obscuring instructions stored in obscuring instruction bank, and transformation functions from the transformation function bank, and applying said selected transformation functions to transform the selected obscuring instruction identification codes and employ the transformed obscuring instruction identification codes to generate additional obscuring instructions (see the method of choosing mutations by cycling through the pseudo-random keys in column 5, lines 38-46).

Claim Rejections - 35 USC § 103

14. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

15. Claims 6-7, 20, 24, 27 rejected under 35 U.S.C. 103 (a) as being unpatentable over Aucsmith et al (US5892899) as applied respectively to claims 1, 19, and 21 above,

and further in view of Pendakur (US006502126B1). Aucsmith et al discloses that said injecting comprises systematically injecting the second obscuring instructions forming a plurality of obscured instruction blocks, each comprising one or more of the serialized sequence of instructions, and one or more of the second obscuring instructions wherein said serialized sequence of instructions, said second obscuring instructions, and the resulting obscured instruction blocks are in source form, and the method further comprises obscurely compiling the obscured instruction blocks into object form, preserving the obscuration (Aucsmith et al - column 1, lines 46-57; column 4, lines 16-20; column 5, lines 38-46; column 7, lines 9-15 and 23-25; column 10, lines 62-65; column 11, lines 42-47 and lines 66-67; column 12, lines 1-3). Aucsmith et al does not expressly disclose a runtime manager. However, Pendakur discloses this feature (Pendakur - abstract; Fig. 3 – elements 40a, 40b, and associated text; column 1, line 60 to column 3, line 5). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to include the runtime manager among the data with which the second obscuring instructions are injected. One of ordinary skill in the art would have been motivated to do so in order to make a security-sensitive runtime manager tamper resistant through an obfuscation method (Aucsmith et al - abstract).

16. Claims 10-13, 17, and 22-23 rejected under 35 U.S.C. 103(a) as being unpatentable over Aucsmith et al (US5892899) as applied respectively to claims 1 and 10 above, and further in view of Bellare et al (US5673319A).

17. As per claims 10-13, in addition to the teachings applied above, Aucsmith et al discloses the preparation of first obscuring data (column 1, lines 46-57; column 4, lines

16-20; column 5, lines 38-46; column 7, lines 9-15 and 23-25), the injection of second obscuring data into a plurality of locations in the data file using an automated process and the first obscuring data . . . (column 1, lines 46-57; column 4, lines 16-20; column 5, lines 38-46; column 7, lines 9-15 and 23-25), and the encryption of the obscured data blocks into a plurality of encrypted obscured data blocks (column 10, lines 62-65). These steps are taught as being combined on a computer system and an embedded controller in two example embodiments (column 11, lines 42-47 and lines 66-67; column 12, lines 1-3), and this office action interprets the obscured data generated as comprising the data taught in all of these steps combined. Aucsmith et al fails to expressly disclose that the encrypted obscured data blocks are successively nested. However, Bellare et al discloses this feature (Bellare et al, column 1, lines 48-60; column 2, 42-45; and claim 3). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Aucsmith et al by encrypting the obscured data blocks in successively nested manner as per the teachings of Bellare et al. One of ordinary skill in the art would have been motivated to do so in order to order to more effectively hide or secure the obscured data blocks from malicious users (see Bellare et al, column 1, lines 10-26, 37-40, 48-60 and column 2, lines 42-45).

18. As per claim 17, in addition to the teachings applied above, Aucsmith et al further discloses the compression of the data or instructions being encrypted (Aucsmith et al, column 6, lines 57-64).

19. As per claims 22 and 23, in addition to the teachings applied above, Aucsmith et al, in a second aspect of a tamper resistant method, discloses the following:

loading a first executable instruction block of an executable module, the first executable instruction block having one or more of the critical instructions, and the executable module further having a plurality of encrypted executable instruction blocks having the remaining of the critical instructions that were generated through encryption ("security sensitive program" in column 5, lines 20-22; "subprograms" and "executions" in column 5, lines 30-34; "jump block" in column 6, lines 19-22; column 7; lines 16-25; Figure 4 - elements 201, 202, 204, and associated text; Figure 5, element 209 and associated text);

executing the loaded first executable instructions block, including loading the plurality of encrypted executable instruction blocks having a first remainder of the critical instructions, retrieving a first decryption key from the loaded plurality of encrypted executable instruction blocks, decrypting the loaded plurality of encrypted executable instruction blocks once to recover a second executable instruction block and a first remainder of the plurality of encrypted executable instruction blocks having a second remainder of the critical instructions ("security sensitive program" in column 5, lines 20-22; "subprograms" and "executions" in column 5, lines 30-34; "jump block" in column 6, lines 19-22; column 7; lines 16-25; Figure 4 - elements 201, 202, 204, and associated text; Figure 5, element 209 and associated text);

executing the second executable instruction block . . . ("security sensitive program" in column 5, lines 20-22; "subprograms" and "executions" in column 5, lines

30-34; "jump block" in column 6, lines 19-22; column 7; lines 16-25; K_p^{pvt},K_c, decryption of Kp^{pub}[Kc], and decryption of Kc[cntnt] in column 11, lines 13-24; "using its own" in column 11, line 18 and "recovered" in column 11, lines 22-23; Figure 4 - elements 201, 202, 204, and associated text; Figure 5, element 209 and associated text).

Aucsmith et al fails to expressly disclose that the encrypted executable instruction blocks are successively nested. However, Bellare et al discloses this feature (Bellare et al, column 1, lines 48-60; column 2, 42-45; and claim 3). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Aucsmith et al by encrypting the executable instruction blocks in a successively nested manner as per the teachings of Bellare et al. One of ordinary skill in the art would have been motivated to do so in order to order to more effectively hide or secure the encrypted executable instruction blocks from malicious users (see Bellare et al, column 1, lines 10-26, 37-40, 48-60 and column 2, lines 42-45).

20. Claims 8-9 and 25-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Aucsmith et al (US5892899) as applied to claims 1 and 19 above, in view of Pendakur (US006502126B1) as applied respectively to claims 7 and 24 above, and further in view of Bellare et al (US5673319A). According to the teachings applied above and in addition to the other teachings applied above, Aucsmith et al discloses the encryption of the obscured data blocks into a plurality of encrypted obscured data blocks (column 10, lines 62-65) but fails to expressly disclose that the encryption occurs successively and recursively, encrypting up to all, except a root one, of the obscured instruction blocks in object form, to form an obscured executable image having the

encrypted ones of the obscured instruction blocks in object form successively nested. However, Bellare et al discloses these features in a Cipher Block Chaining encryption algorithm (Bellare et al, column 1, lines 48-60; column 2, 42-45; and claim 3). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Aucsmith et al by successively and recursively encrypting up to all, except a root one, of the obscured instruction blocks in object form, to form an obscured executable image having the encrypted ones of the obscured instruction blocks in object form successively nested by using the cipher block chaining encryption algorithm disclosed in Bellare et al. One of ordinary skill in the art would have been motivated to do so in order to to more effectively hide or secure the obscured data blocks from malicious users (see Bellare et al, column 1, lines 10-26, 37-40, 48-60 and column 2, lines 42-45).

Conclusion

21. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to James Curcio whose telephone number is 703-305-8887. The examiner can normally be reached on Tuesday to Friday from 7 am to 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron, can be reached on Monday to Thursday from 7:30 am to 4:30 pm. The examiner's supervisor may also be reached on alternate Fridays from 7:30 am to 4:30 pm. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

JC

GILBERTO BARRÓN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

June 14, 2004
JC
AU 2132